IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Divisional Application of

KATO et al. Group Art Unit: 2132

Appln. No.: Not Yet Assigned Examiner: D. Meislahn

Filed: January 4, 2002

FOR: METHOD AND APPARATUS OF ENCIPHERING AND DECIPHERING DATA USING MULTIPLE KEYS

* * * * *

January 4, 2002

FIRST PRELIMINARY AMENDMENT TO BE ENTERED PRIOR TO FILING FEE CALCULATON PER PARAGRAPH 14 OF REQUEST FOR FILING

Hon. Commissioner of Patents
Washington, DC 20231

Sir:

Before beginning examination, please amend the above-identified application as follows:

IN THE CLAIMS:

Please cancel claims 2-22.

Respectfully submitted,

PILLSBURY WINTHROP LLP

Dale Lazar
Reg. No. 28872
Phone: (703) 905-2126
Fax: (703) 905-2500

DSL/jrh

1600 Tysons Boulevard
McLean, VA 22102
(703) 905-2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Divisional Application of

KATO et al. Group Art Unit: 2132

Appln. No.: Not Yet Assigned Examiner: D. Meislahn

Filed: January 4, 2002

FOR: METHOD AND APPARATUS OF ENCIPHERING AND DECIPHERING DATA USING MULTIPLE KEYS

* * * * *

January 4, 2002

SECOND PRELIMINARY AMENDMENT TO BE ENTERED AFTER FILING FEE CALCULATION PER PARAGRAPH 24 OF REQUEST FOR FILING

Hon. Commissioner of Patents
Washington, DC 20231

Sir:

Before beginning examination, please amend the above-identified application as follows:

IN THE TITLE:

Please change the title of the above-identified application to

--METHOD AND APPARATUS OF ENCIPHERING AND DECIPHERING DATA USING KEYS ENCIPHERED AND DECIPHERED WITH OTHER KEYS--.

IN THE SPECIFICATION:

On page 1, just after the title, please insert the following paragraph:

--This is a divisional application of U.S. Patent Application No. 08/883,337, filed on June 26, 1997, which is incorporated by reference in its entirety.--

Page 15, please replace the paragraph beginning with line 19 with the following paragraph:

--In the embodiments, explanation will be given using an example of a system that reads the image data compressed and enciphered according to the MPEG 2 data compression standard from a DVD and enciphers, decodes, and reproduces the read-out data.--

Page 19, please replace the paragraph beginning with line 21 with the following paragraph:

-- As for the timing of generating random numbers (e.g., the timing of inputting time information), for example, the timing with which the signal indicating that the DVD 101 has been loaded into the DVD driving unit is asserted may be used.--

Page 21, please replace the paragraph beginning with line 12 with the following paragraph:

-- At step S7, the deciphering circuit 112 of the deciphering unit 114 deciphers E_{SK}(Data) received via the CPU BUS 110 using the first session key S_K and produces:

D_{SK} (E_{SK} (Data)) -= Data--

Page 22, please replace the paragraph beginning at line 17 with the following paragraph:

--As described above, with the first embodiment, when the data is reproduced from a medium on which the digitized data has been enciphered and recorded (when the enciphered data is deciphered), the deciphered data is prevented from flowing over the CPU BUS of the computer and the second session key $S_{K'}$ used to encipher the first session key necessary for deciphering the enciphered data flowing over the CPU BUS is created on the basis of

information that changes each time the data is reproduced, such as time information. Therefore, even when the data flowing the CPU BUS 110 is stored from signal lines 210 into a digital storage medium 211 as shown in Fig. 4, the data cannot be reproduced or used.--

Page 27, please replace the paragraph beginning with line 3 with the following paragraph:

--In the second embodiment, there is an n number of types of master keys. A first session key is represented by S_K, a second session key by $S_{K'}$, the t-th master key M_{Kt} (t is in the range of 1 to n), and image data (i.e., the data to be enciphered) Data.--

Page 28, please replace the paragraphs beginning with lines 2, 6, 11, 20 and 25 with the following paragraphs, respectively:

--(Method 1) One session key $E_{MKi}(S_K)$ (i is in the range of 1 to n) is recorded n the DVD 101. The deciphering unit 114a has an n number of master keys M_{Kj} (j = 1 to n) in it.--

--(Method 2) An n number of session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded n the DVD 101. The deciphering unit 114a has one master key M_{Kj} (j is in the range of 1 to n) in it.--

--(Method 3) This is an expansion of Method 2. An n number of session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on the DVD 101. The deciphering unit 114a has an m ($2 < m < n$) number of master keys M_{Kj} (j = 1 to n) in it. The m number of master keys have been selected from the n number of master keys beforehand.--

--(Method 4) This is the reverse of Method 3. An m ($2 < m < n$) number of session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on the DVD 101. The m number of master keys have been selected from an n number of master keys M_{Kj} (j = 1 to n) beforehand. The deciphering unit 114a has an n number of master keys M_{Kj} (j = 1 to n) in it.--

--(Method 5) An n number of session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on the DVD 101. The deciphering unit 114a has an n number of master key M_{Kj} (j = 1 to n) in it.--

Page 29, please replace the paragraph beginning at line 19 with the following paragraph:

--A predetermined master key is assumed to have been registered in the enciphering unit 107.--

Page 34, please replace the paragraph beginning at line 1 with the following paragraph:

--The fourth line in the procedure indicates the operation of judging whether or not DS1[i] coincides with DS2[i].--

Page 35, please replace the paragraph beginning with line 4 with the following paragraph:

--At step S21, the deciphering circuit 112 of the deciphering unit 114a deciphers E_{SK}(Data) received via the CPU Bus 110 using the first session key S_K and produces:

D_{SK} (E_{SK} (Data)) = Data--

Page 36, please replace the paragraph beginning with line 11 with the following paragraph:

--As described above, with the second embodiment, even when the data flowing over the CPU BUS 110 is stored, the data cannot be reproduced or used, as in the first embodiment.--

Page 38, please replace the paragraph beginning at line 24 with the following paragraph:

--As for the time of generating random numbers (e.g., the timing of inputting time information), for example, the timing with which the signal indicating that the DVD 101 has been loaded into the DVD driving unit is asserted may be used.--

Page 47, please replace the paragraphs beginning with lines 10, 19 and 24 with the following paragraphs, respectively:

--For example, when the same master keys as that registered in the deciphering unit 114a are also registered in the enciphering unit 107, the operation is the same as of that of Method 5.--

--In these cases, however, in the procedure of each of Method 1 to Method 5, enciphering is replaced with deciphering. Specifically, $D_{MKj}(S_{K'})$ and $D_{SK'}(S_{K'})$ are transferred from the deciphering unit 114a to the enciphering unit 107.--

--In addition to the configuration using the master key, various suitable configurations may be used as the configuration that safely transfers the second session key $S_{K'}$ from the deciphering unit 114a to the enciphering unit 107 over the CPU BUS 110, such as the techniques disclosed in Nikkei Electronics, No. 676, Nov. 18, 1996, pp. 13-14. In this case, it is not necessary to register a master key in the enciphering unit 107.--

Page 58, please replace the paragraph beginning with line 23 with the following paragraph:

--Explanation will be given about a case where an n number of session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on a DVD. A DVD player (a deciphering unit 114b) has an m ($2 < m < n$) number of master keys M_{Kj} (j is in the range of 1 to n) in it. The m number of master

keys have been selected from the n number of master keys beforehand. The master keys M_{Kj} are assumed to be allocated exclusively to the DVD player maker. It is assumed that n = 100 and m -= 10.--

IN THE CLAIMS:

Please cancel claim 1 and add new claims 23-47.

23. (New) An enciphering method comprising:

keeping a plurality of second keys;

enciphering data with a first key; and

enciphering said first key with a p number of second keys, where p is an integer greater than or equal to two, of the kept plurality of second keys to obtain a p number of enciphered first keys, respectively.

24. (New) An enciphering method according to claim 23, wherein said data includes at least one of key information, documents, sound, images, and programs.

25. (New) An enciphering method according to claim 23, further comprising:

selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken.

26. (New) A recording medium having information items recorded thereon, said information items comprising:

first information composed of enciphered data obtained by enciphering data with a first key; and

second information composed of a p number enciphered first keys, where p is an integer greater than or equal to two, obtained by enciphering said first key with a p number of second keys, respectively,

wherein said second information composed of the p number of enciphered first keys is recorded in a key recording area of said recording medium.

27. (New) A recording medium according to claim 26, wherein said recording medium is a removable recording medium.

28. (New) A recording medium manufacturing method comprising:

keeping a plurality of second keys;

obtaining first information composed on enciphered data by enciphering data with a first key;

obtaining second information composed of a p number of enciphered first keys, where p is an integer greater than or equal to two, obtained by enciphering said first key with a p number of second keys of the kept plurality of second keys, respectively; and

recording said first and second information on the same recording medium.

29. (New) A recording medium manufacturing method according to claim 28, further comprising:

selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken.

30. (New) A recording medium manufacturing method according to claim 28, further comprising:

recording said second information composed of the p number of enciphered first keys in a key recording area of said recording medium.

31. (New) A recording medium manufacturing method according to claim 30, wherein said recording medium is a removable recording medium.

32. (New) A deciphering method comprising:

recording at least part of a p number of second keys, where p is an integer geater than or equal to two, in a secret area;

inputting first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering said first key with said p number of second keys, respectively;

deciphering at least one said p number of enciphered first keys using the recorded at least part of the p number of second keys to obtain said first key;

confirming by a specific method that the obtained first key is correct; and

deciphering said enciphered data using said obtained first key after the confirmation to obtain said data.

33. (New) A deciphering method according to claim 32, wherein said data includes at least one of key information, documents, sound, images, and programs.

34. (New) A deciphering device comprising:

a recording unit configured to record at least part of a p number of second keys, where p is an integer greater than or equal to two, in a secret area;

an input unit configured to input first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering said first key with said p number of second keys, respectively; and

a deciphering unit configured to decipher at least one of said p number of enciphered first keys of said second information inputted from said input unit using the recorded at least part of the p number of second keys in said recording unit, confirm by a specific method that the obtained first key is correct, and decipher said enciphered data of said first information using said first key after the confirmation to obtain said data.

35. (New) A recording and reproducing device comprising:

a recording unit configured to record at least part of a p number of second keys, where p is an integer greater than or equal to two, in a secret area;

a reading unit configured to read first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering said first key with a p number of second keys from a recording medium on which said first information and said second information have been stored, respectively, and

a deciphering unit configured to decipher at least one of said p number of enciphered first keys of said second information read by said reading unit using the recorded at least part of the p number of second keys in said storage unit, confirm by a specific method that the obtained first key is correct, and decipher said enciphered data of said first information using said first key after the confirmation to obtain said data.

36. (New) A key control method comprising:

causing a first caretaker to take custody of a plurality of second keys;

causing a second caretaker to take custody of first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys, where p is an integer greater than or equal to two, obtained by enciphering said first key with a p number of second keys of said plurality of second keys, respectively, and

causing a third caretaker to take custody of at least part of said plurality of second keys, said at least part of said plurality of second keys being recorded in a secret area of a device provided by said third caretaker.

37. (New) An enciphering method comprising:

keeping a plurality of second keys;

enciphering data with a first key;

enciphering said first key with a p number of second keys, where p is an integer greater than or equal to two, of the kept plurality of second keys to obtain a p number of enciphered first keys, respectively, and

recording the enciphered data and the p number of enciphered first keys on a recording medium to be distributed to a user.

38. (New) An enciphering method according to claim 37, further comprising:

selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken.

39. (New) An enciphering method according to claim 37, further comprising:

recording the p number of enciphered first keys in a key recording area of said recording medium.

40. (New) An enciphering method according to claim 39, wherein said recording medium is a removable recording medium.

41. (New) A master key control method comprising:

keeping a plurality of master keys;

allocating at least part of the plurality of master keys to said player maker;

receiving a session key supplied from a disk maker;

selecting part of the plurality of master keys for use in enciphering said session key in a case where part of the plurality of master keys has been broken;

enciphering the received session key with the selected part of the plurality of master keys to produce a plurality of enciphered session keys, respectively; and

supplying the produced plurality of enciphered session keys to said disk maker.

42. (New) An enciphering method comprising:

keeping a plurality of second keys;

enciphering data with a first key;

enciphering said first key with a p number of second keys, where p is an integer greater than or equal to two, of the kept plurality of second keys to obtain a p number of enciphered first keys, respectively; and

enciphering said first key with said first key itself.

43. (New) A key control method applied to a key control organization, a disk maker, and a player maker, said method comprising:

taking custody of a plurality of master keys by said key control organization, wherein said key control organization allocates part of the plurality of master keys to said player maker, receives a session key supplied from said disk maker, enciphers the received session key with said plurality of master keys to produce first information composed of a plurality of enciphered session keys, respectively, and supplies the produced first information to said disk maker;

providing a player device by said player maker, said player device having one or more master keys that are allocated by said key control organization; and

providing a disk by said disk maker, wherein said disk maker produces the session key and supplies the produced session key to said key control organization, receiving the first information supplied from said key control organization, acquiring second information obtained by enciphering the session key with itself and third information obtained by enciphering data with the session key, and recording the first information, the second information, and the third information onto said disk.

44. (New) A key control method according to claim 43, wherein said key control organization allocates a different part of the plurality of master keys exclusively to a plurality of player makers.

45.(New) A key control method according to claim 43, wherein in a case where a master key has been broken, said disk maker manufactures a disk without using the broken master key.

46. (New) A disk manufacturing method comprising:

producing a session key;

enciphering data with the session key to obtain first information;

supplying the session key to a key control organization;

producing second information by enciphering the produced session key with itself;

receiving from said key control organization, third information composed of a plurality of enciphered session keys obtained by enciphering the supplied session key with a plurality of master keys, respectively; and

recording the first information, the second information, and the third information onto a recording mechanism.

47. (New) A disk manufacturing method comprising:

producing a session key;

enciphering data with the session key to obtain first information;

supplying the session key to a key control organization;

received from said key control organization, second information obtained by enciphering the supplied session key with itself;

receiving from said key control organization, third information composed of a plurality of enciphered session keys obtained by enciphering the supplied session key with a plurality of master keys, respectively, and

recording the first information, the second information, and the third information onto a recording medium.

REMARKS

This is a divisional application from U.S. Application Serial No. 08/883,337.

By this amendment, claim 1 has been canceled and new claims 23-47 have been added. No new matter has been added to the application. An early action on the merits and the allowance of all claims are earnestly solicited.

Also enclosed is a Drawing Change Authorization Request to correct typographical errors in Figs. 7 and 10. No new matter has been added.

Attached hereto is a marked-up version of the changes made to the title and the specification by the current amendment. The attached Appendix is captioned **"VERSION WITH MARKINGS TO SHOW CHANGES MADE"**.

Respectfully submitted,

PILLSBURY WINTHROP LLP

Dale Lazar
Reg. No. 28872
Phone: (703) 905-2126
Fax: (703) 905-2500

DSL/jrh

1600 Tysons Boulevard
McLean, VA 22102
(703) 905-2000

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE TITLE:

Please change the title of the above-identified application to

--METHOD AND APPARATUS OF ENCIPHERING AND DECIPHERING DATA USING [MULTIPLE] KEYS ENCIPHERED AND DECIPHERED WITH OTHER KEYS--.

IN THE SPECIFICATION:

Page 15, please replace the paragraph beginning with line 19 with the following paragraph:

--In the embodiments, explanation will be given using an example of a system that reads the image data compressed and enciphered according to the MPEG 2 data compression standard from a DVD and enciphers, decodes, and reproduces the read-out data.--

Page 19, please replace the paragraph beginning with line 21 with the following paragraph:

-- As for the timing of generating random numbers (e.g., the timing of inputting time information), for example, the timing with which the signal indicating that the DVD 101 has been loaded into the DVD driving unit is asserted may be used.--

Page 21, please replace the paragraph beginning with line 12 with the following paragraph:

-- At step S7, the deciphering circuit 112 of the deciphering unit 114 deciphers E_{SK}(Data) received via the CPU BUS 110 using the first session key S_K and produces:

D_{SK} (E_{SK} (Data)) -= Data--

Page 22, replace the paragraph beginning at line 17 with the following paragraph:

--As described above, with the first embodiment, when the data is reproduced from a medium on which the digitized data has been enciphered and recorded (when the enciphered data is deciphered), the deciphered data is prevented from flowing over the CPU BUS of the computer and the second session key $S_{K'}$ used to encipher the first session key necessary for deciphering the enciphered data flowing over the CPU BUS is created on the basis of information that changes each time the data is reproduced, such as time information. Therefore, even when the data flowing the CPU BUS 110 is stored from signal lines 210 into a digital storage medium 211 as shown in Fig. 4, the data cannot be reproduced [of] or used.--

Page 27, please replace the paragraph beginning with line 3 with the following paragraph:

--In the second embodiment, there is an n number of types of master keys. A first session key is represented by S_K, a second session key by $S_{K'}$, the [n] t-th master key M_{Kt} ([t s] t is in the range of 1 to n), and image data (i.e., the data to be enciphered) Data.--

Page 28, please replace the paragraphs beginning with lines 2, 6, 11, 20 and 25 with the following paragraphs, respectively:

--(Method 1) One [master] session key $E_{MKi}(S_K)$ (i is in the range of 1 to n) is recorded n the DVD 101. The deciphering unit 114a has an n number of master keys M_{Kj} (j = 1 to n) in it.--

--(Method 2) An n number of [master] session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded n the DVD 101. The deciphering unit 114a has one master key M_{Kj} (j is in the range of 1 to n) in it.--

--(Method 3) This is an expansion of Method 2. An n number of [master] session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on the DVD 101. The deciphering unit 114a has an m ($2 < m < n$) number of master keys M_{Kj} (j = 1 to n) in it. The m number of master keys have been selected from the n number of master keys beforehand.--

--(Method 4) This is the reverse of Method 3. An m ($2 < m < n$) number of [master] session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on the DVD 101. The m number of master keys have been selected from an n number of master keys M_{Kj} (j = 1 to n) beforehand. The deciphering unit 114a has an n number of master keys M_{Kj} (j = 1 to n) in it.--

--(Method 5) An n number of [master] session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on the DVD 101. The deciphering unit 114a has an n number of master key M_{Kj} (j = 1 to n) in it.--

Page 29, please replace the paragraph beginning at line 19 with the following paragraph:

--A predetermined master key is assumed to have been registered in the [deciphering] enciphering unit 107.--

Page 34, please replace the paragraph beginning at line 1 with the following paragraph:

--The fourth line in the procedure indicates the operation of judging whether [nor] or not DS1[i] coincides with DS2[i].--

Page 35, please replace the paragraph beginning with line 4 with the following paragraph:

--At step S21, the deciphering circuit 112 of the deciphering unit 114a deciphers E_{SK}(Data) received via the CPU Bus 110 using the first session key S_K and produces:

D_{SK} (E_{SK} (Data)) = Data--

Page 36, please replace the paragraph beginning with line 11 with the following paragraph:

--As described above, with the second embodiment, even when the data flowing over the CPU BUS 110 is stored, the data cannot be reproduced [of] or used, as in the first embodiment.--

Page 38, please replace the paragraph beginning at line 24 with the following paragraph:

--As for the time of generating random numbers (e.g., the timing of inputting time information), for example, the timing with which the signal indicating that the DVD 101 has been loaded into the DVD driving unit is asserted may be used.--

Page 47, please replace the paragraphs beginning with lines 10, 19 and 24 with the following paragraphs, respectively:

--For example, when the same master keys as that registered in the deciphering unit 114a [is] are also registered in the enciphering unit 107, the operation is the same as of that of Method 5.--

--In these cases, however, in the procedure of each of Method 1 to Method 5, enciphering is replaced with deciphering. Specifically, [$D_{Mki}(S_K)$ and $D_{SK}(S_K)$] $D_{MKi}(S_{K'})$ and $D_{SK'}(S_{K'})$ are transferred from the deciphering unit 114a to the enciphering unit 107.--

--In addition to the configuration using the master key, various suitable configurations may be used as the configuration that safely transfers the second session key $S_{K'}$ from the deciphering unit 114a to the enciphering unit 107 over the CPU BUS 110[. For example,], such as the techniques disclosed in Nikkei Electronics, No. 676, Nov. 18, 1996, pp. 13-14. In this case, it is not necessary to register a master key in the enciphering unit 107.--

Page 58, please replace the paragraph beginning with line 23 with the following paragraph:

--Explanation will be given about a case where an n number of [master] session keys $E_{MKi}(S_K)$ (i = 1 to n) are recorded on a DVD. A DVD player (a deciphering unit 114b) has an m ($2 < m < n$) number of master keys M_{Kj} (j is in the range of 1 to n) in it. The m number of master keys have been selected from the n number of master keys beforehand. The master keys M_{Kj} are assumed to be allocated exclusively to the DVD player maker. It is assumed that n = 100 and m -= 10.--

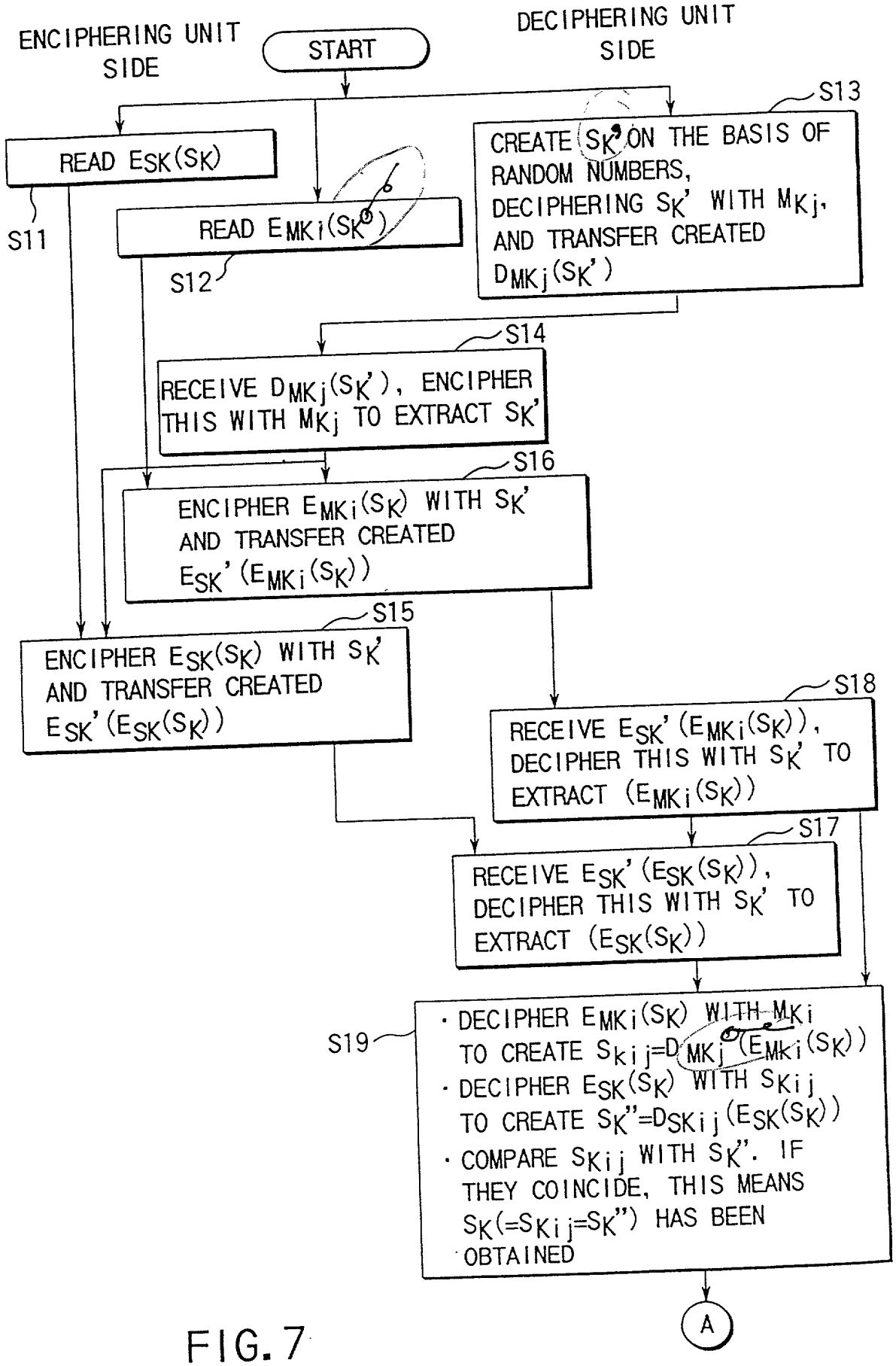
ENCIPHERING UNIT SIDE
START
DECIPHERING UNIT SIDE
READ $E_{SK}(S_K)$
S11
READ $E_{MKi}(S_K)$
S12
S13
CREATE S_K' ON THE BASIS OF RANDOM NUMBERS, DECIPHERING S_K' WITH M_{Kj}, AND TRANSFER CREATED $D_{MKj}(S_K')$
S14
RECEIVE $D_{MKj}(S_K')$, ENCIPHER THIS WITH M_{Kj} TO EXTRACT S_K'
S16
ENCIPHER $E_{MKi}(S_K)$ WITH S_K' AND TRANSFER CREATED $E_{SK}'(E_{MKi}(S_K))$
S15
ENCIPHER $E_{SK}(S_K)$ WITH S_K' AND TRANSFER CREATED $E_{SK}'(E_{SK}(S_K))$
S18
RECEIVE $E_{SK}'(E_{MKi}(S_K))$, DECIPHER THIS WITH S_K' TO EXTRACT $(E_{MKi}(S_K))$
S17
RECEIVE $E_{SK}'(E_{SK}(S_K))$, DECIPHER THIS WITH S_K' TO EXTRACT $(E_{SK}(S_K))$
S19
· DECIPHER $E_{MKi}(S_K)$ WITH M_{Ki} TO CREATE $S_{Kij}=D_{MKj}(E_{MKi}(S_K))$
· DECIPHER $E_{SK}(S_K)$ WITH S_{Kij} TO CREATE $S_K''=D_{SKij}(E_{SK}(S_K))$
· COMPARE S_{Kij} WITH S_K''. IF THEY COINCIDE, THIS MEANS $S_K(=S_{Kij}=S_K'')$ HAS BEEN OBTAINED
A

FIG. 7

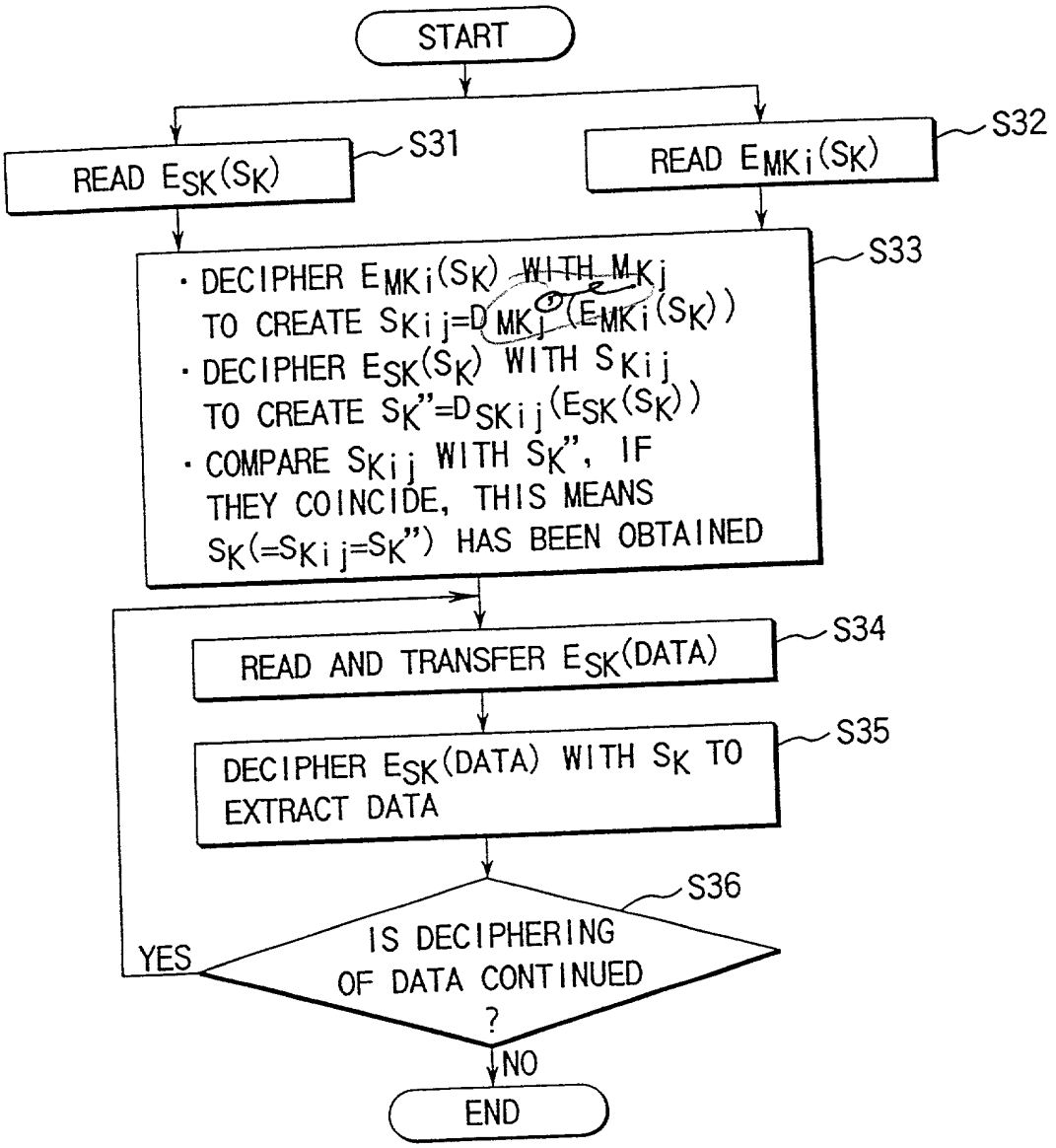
START
READ $E_{SK}(S_K)$
S31
READ $E_{MKi}(S_K)$
S32
· DECIPHER $E_{MKi}(S_K)$ WITH M_{Kj} TO CREATE $S_{Kij}=D_{MKj}(E_{MKi}(S_K))$
· DECIPHER $E_{SK}(S_K)$ WITH S_{Kij} TO CREATE $S_K''=D_{SKij}(E_{SK}(S_K))$
· COMPARE S_{Kij} WITH S_K'', IF THEY COINCIDE, THIS MEANS $S_K(=S_{Kij}=S_K'')$ HAS BEEN OBTAINED
S33
READ AND TRANSFER $E_{SK}(DATA)$
S34
DECIPHER $E_{SK}(DATA)$ WITH S_K TO EXTRACT DATA
S35
IS DECIPHERING OF DATA CONTINUED ?
S36
YES
NO
END

FIG. 10